BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平11－53185

(43)公開日　平成11年(1999)２月26日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｚ
15/00	３３０	15/00	３３０Ｚ

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）

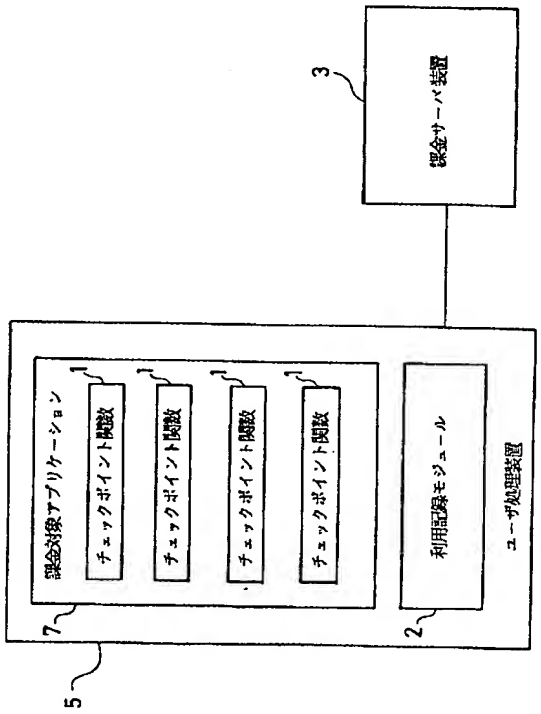
(21)出願番号　特願平9－206493

(22)出願日　平成９年(1997)７月31日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　田中　利清
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　弁理士　三好　秀和　(外１名)

(54)【発明の名称】　プログラムの機能単位利用量課金方法

(57)【要約】
【課題】　ソフトウエアの使用機能に対応し、使用回数に比例した使用料の徴収を可能にするプログラムの機能単位利用量課金方法を提供する。
【解決手段】　課金対象アプリケーションの実行に先立ち、利用記録モジュール２はアプリケーション使用要求を課金サーバ装置３に送信し、課金サーバ装置は暗号鍵Ｋを利用記録モジュール２に送信し、課金対象アプリケーションの実行時にはチェックポイント関数１は起動毎に乱数R_1を生成し、該乱数を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールは起動通知の回数を更新し、暗号鍵Ｋを用いて前記チェックポイント関数からの乱数R_1を暗号化し、この暗号化乱数をチェックポイント関数に返却し、チェックポイント関数は復号鍵Ｋ’を用いて利用記録モジュールからの暗号化乱数Ｋ（R_1）を復号化し、乱数R_1’とR_1の一致を検証する。



1

【特許請求の範囲】

【請求項１】　課金対象アプリケーションを有するユーザ処理装置に設けられた利用記録モジュールおよび前記ユーザ処理装置とネットワークを介して接続された課金サーバ装置を有するプログラム課金システムにおいて、

課金対象アプリケーションは予め課金対象機能単位毎にチェックポイント関数が埋め込まれて配布され、

前記チェックポイント関数は起動される毎に起動通知を前記利用記録モジュールへ通知し、

前記利用記録モジュールは前記起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを特徴とするプログラムの機能単位利用量課金方法。

【請求項２】　前記チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、

前記利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを特徴とする請求項１記載のプログラムの機能単位利用量課金方法。

【請求項３】　前記チェックポイント関数は起動される毎に単価を添付した起動通知を前記利用記録モジュールに通知し、

前記利用記録モジュールは単価の累積を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを特徴とする請求項１または２記載のプログラムの機能単位利用量課金方法。

【請求項４】　前記チェックポイント関数には予め復号鍵Ｋ’が埋め込まれ、

前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールはアプリケーション使用要求を前記課金サーバ装置に送信し、

前記課金サーバ装置は前記復号鍵Ｋ’に対応する暗号鍵Ｋを前記利用記録モジュールに送信し、

前記利用記録モジュールは前記課金サーバ装置から受信した前記暗号鍵Ｋを保持し、

前記課金対象アプリケーションの実行時において、前記チェックポイント関数は起動される毎に乱数R_1を生成し、この生成した乱数R_1を添付した起動通知を前記利用記録モジュールに通知し、

前記利用記録モジュールは起動通知の回数を更新保持し、前記暗号鍵Ｋを用いて前記チェックポイント関数から受け取った前記乱数R_1を暗号化し、この暗号化した乱数Ｋ（R_1）を前記チェックポイント関数に返却し、

前記チェックポイント関数は前記復号鍵Ｋ’を用いて前記利用記録モジュールから返却された前記暗号化された乱数Ｋ（R_1）を復号化し、この復号化した乱数R_1’と前記生成された乱数R_1が一致していることを検証し、

前記利用記録モジュールは保持した利用記録を前記課金サーバ装置に転送することを特徴とする請求項１乃至３のいずれかに記載のプログラムの機能単位利用量課金方法。

2

【請求項５】　前記チェックポイント関数には予め復号鍵Ｋ’が埋め込まれ、

前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールは前記課金対象アプリケーションのプログラム識別情報を添付して、アプリケーション使用要求を前記課金サーバ装置に送信し、

前記課金サーバ装置は前記プログラム識別情報で指定された前記課金対象アプリケーションに埋め込まれた前記復号鍵Ｋ’に対応する暗号鍵Ｋを前記利用記録モジュールに送信し、

前記利用記録モジュールは前記課金サーバ装置から受信した前記暗号鍵Ｋを前記プログラム識別情報と対にして保持し、

前記課金対象アプリケーションの実行時において、前記チェックポイント関数は起動される毎に乱数R_1を生成し、この生成した乱数R_1と課金対象アプリケーションのプログラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、

前記利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新保持し、前記プログラム識別情報に対応して前記暗号鍵Ｋを用いて前記チェックポイント関数から受け取った前記乱数R_1を暗号化し、この暗号化した乱数Ｋ（R_1）を前記チェックポイント関数に返却し、

前記チェックポイント関数は前記復号鍵Ｋ’を用いて前記利用記録モジュールから返却された前記暗号化された乱数Ｋ（R_1）を復号化し、この復号化した乱数R_1’と前記生成された乱数R_1が一致していることを検証し、

前記利用記録モジュールは保持した利用記録を前記課金サーバ装置に転送することを特徴とする請求項１乃至３のいずれかに記載のプログラムの機能単位利用量課金方法。

【請求項６】　前記利用記録モジュールは前記課金サーバ装置の公開鍵Ｋｓを保持し、また前記課金サーバ装置は課金サーバ装置自身の私的鍵Ks^{-1}を保持し、

前記利用記録モジュールは利用限度を保持し、前記チェックポイント関数の起動回数または単価累積が利用限度に到達すると、乱数R_2を生成し、この生成した乱数R_2と利用記録Ｕを前記課金サーバ装置の公開鍵Ｋｓを用いて暗号化し、この暗号化した情報Ｋｓ（R_2，Ｕ）を前記課金サーバ装置に送信し、

前記課金サーバ装置は前記利用記録モジュールから受信した前記暗号化情報Ｋｓ（R_2，Ｕ）を前記課金サーバ装置自身の私的鍵Ks^{-1}を用いて復号して前記乱数R_2と利用記録Ｕを抽出し、前記課金サーバ装置が保持する課金情報を更新し、前記乱数R_2を前記課金サーバ装置

自身の私的鍵Ｋｓ$^{-1}$を用いて暗号化し、この暗号化した乱数Ｋｓ$^{-1}$（Ｒ$_2$）を前記利用記録モジュールへ送信し、

前記利用記録モジュールは前記課金サーバ装置から受信した前記暗号化乱数Ｋｓ$^{-1}$（Ｒ$_2$）を前記課金サーバ装置の公開鍵Ｋｓを用いて復号し、この復号した乱数Ｒ$_2$'と前記生成した乱数Ｒ$_2$が一致していることを検証し、前記利用記録モジュール内に保持していた利用記録を削除することを特徴とする請求項１乃至３のいずれかに記載のプログラムの機能単位利用量課金方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＣＤ・ＲＯＭやフロッピーディスク等の媒体に格納されて配布されるソフトウエアや、ネットワークを介して配布されるソフトウエアに対して、機能単位の利用量に基づいて課金を行うプログラムの機能単位利用量課金方法に関する。

【０００２】

【従来の技術】従来のソフトウエア課金システムには、ソフトウエアを販売し、ユーザが当該ソフトウエアを買い取った時点で課金が終了する方法がある。

【０００３】また、ユーザが配布されたソフトウエアを利用する際に、課金センタに使用する旨を通知し、これにより、課金センタでは、ソフトウエアの使用に対する課金を行うシステムがある。

【０００４】また、最近では、買い取り形式として暗号化されたソフトウエアをＣＤ・ＲＯＭ等の媒体、またはネットワーク経由で配布し、電話、ファクシミリ、手紙、または電子メールによる購入手続き後、復号鍵を通知する方式も採用されている。さらに、予め利用可能量が設定され、かつ暗号化されたソフトウエアを配布して、ユーザが使用した量を日数で管理し、当該日数に基づいて課金を行う方法等がある。

【０００５】

【発明が解決しようとする課題】しかしながら、上記の買い取り方式では、流通経費を相対的に低減するためにソフトウエアの機能は肥大化し、ユーザは、殆ど使用しない機能を含め、高額の費用を負担しなければならない。また、ソフトウエアを購入して実行してみなければユーザが必要とする機能が満足されているか否かを判断できない。

【０００６】また、単に、ユーザが配布されたソフトウエアを使用する際に、課金センタに使用する旨を通知する方法では、課金は可能であってもソフトウエアの使用を制限することができないため、使用料金の未払いがあっても対処することができないという問題がある。

【０００７】暗号化されたソフトウエアを予め提供し、使用時に復号鍵を提供するシステムであっても、使用回数に関わらず、ユーザは、同一の金額を支払う必要があり、使用回数、または使用時間当たりの価格には大きな幅がある。

【０００８】本発明は、上記に鑑みてなされたもので、その目的とするところは、ソフトウエアの使用機能に対応し、使用回数に比例した使用料の徴収を可能にするプログラムの機能単位利用量課金方法を提供することにある。

【０００９】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、課金対象アプリケーションを有するユーザ処理装置に設けられた利用記録モジュールおよび前記ユーザ処理装置とネットワークを介して接続された課金サーバ装置を有するプログラム課金システムにおいて、課金対象アプリケーションは予め課金対象機能単位毎にチェックポイント関数が埋め込まれて配布され、前記チェックポイント関数は起動される毎に起動通知を前記利用記録モジュールへ通知し、前記利用記録モジュールは前記起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【００１０】請求項１記載の本発明にあっては、課金対象アプリケーション内に課金対象機能単位毎に予め埋め込まれているチェックポイント関数は起動される毎に起動通知を利用記録モジュールへ通知し、利用記録モジュールは起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するため、課金対象機能単位毎に実行回数に応じた課金が可能である。

【００１１】また、請求項２記載の本発明は、請求項１記載の本発明において、前記チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールがプログラム識別情報毎に起動通知の回数を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【００１２】請求項２記載の本発明にあっては、チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するため、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うことができる。

【００１３】更に、請求項３記載の本発明は、請求項１または２記載の本発明において、前記チェックポイント関数は起動される毎に単価を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールが単価の累積を更新保持し、この保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【００１４】請求項３記載の本発明にあっては、チェッ

クポイント関数は起動される毎に単価を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールは単価の累積を更新し、この利用記録を課金サーバ装置に転送するため、課金対象機能単位毎に単価を設定することにより、課金対象機能単位の開発工数、規模、ノウハウ、難易度、利用価値などにより課金対象機能単位毎に異なる料金を徴収することができる。

【００１５】請求項４記載の本発明は、１乃至３のいずれかに記載の本発明において、前記チェックポイント関数には予め復号鍵Ｋ’が埋め込まれ、前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールがアプリケーション使用要求を前記課金サーバ装置に送信し、前記課金サーバ装置は前記復号鍵Ｋ’に対応する暗号鍵Ｋを前記利用記録モジュールに送信し、前記利用記録モジュールが前記課金サーバ装置から受信した前記暗号鍵Ｋを保持し、前記課金対象アプリケーションの実行時において、前記チェックポイント関数が起動される毎に乱数R_iを生成し、この生成した乱数R_iを添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールが起動通知の回数を更新保持し、前記暗号鍵Ｋを用いて前記チェックポイント関数から受け取った前記乱数R_iを暗号化し、この暗号化した乱数Ｋ（R_i）を前記チェックポイント関数に返却し、前記チェックポイント関数は前記復号鍵Ｋ’を用いて前記利用記録モジュールから返却された前記暗号化された乱数Ｋ（R_i）を復号化し、この復号化した乱数R_i’と前記生成された乱数R_iが一致していることを検証し、前記利用記録モジュールが保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【００１６】請求項４記載の本発明にあっては、チェックポイント関数で起動毎に乱数を生成して利用記録モジュールへ通知し、利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するため、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証することができる。

【００１７】また、請求項５の本発明は、請求項１乃至３のいずれかに記載の本発明において、前記チェックポイント関数には予め復号鍵Ｋ’が埋め込まれ、前記課金対象アプリケーションの実行に先立ち、前記利用記録モジュールが前記課金対象アプリケーションのプログラム識別情報を添付して、アプリケーション使用要求を前記課金サーバ装置に送信し、前記課金サーバ装置が前記プログラム識別情報で指定された前記課金対象アプリケーションに埋め込まれた前記復号鍵Ｋ’に対応する暗号鍵Ｋを前記利用記録モジュールに送信し、前記利用記録モジュールが前記課金サーバ装置から受信した前記暗号鍵Ｋを前記プログラム識別情報と対にして保持し、前記課金対象アプリケーションの実行時において、前記チェックポイント関数が起動される毎に乱数R_iを生成し、この生成した乱数R_iと課金対象アプリケーションのプログラム識別情報を添付した起動通知を前記利用記録モジュールに通知し、前記利用記録モジュールがプログラム識別情報毎に起動通知の回数を更新保持し、前記プログラム識別情報に対応して前記暗号鍵Ｋを用いて前記チェックポイント関数から受け取った前記乱数R_iを暗号化し、この暗号化した乱数Ｋ（R_i）を前記チェックポイント関数に返却し、前記チェックポイント関数が前記復号鍵Ｋ’を用いて前記利用記録モジュールから返却された前記暗号化された乱数Ｋ（R_i）を復号化し、この復号化した乱数R_i’と前記生成された乱数R_iが一致していることを検証し、前記利用記録モジュールが保持した利用記録を前記課金サーバ装置に転送することを要旨とする。

【００１８】請求項５記載の本発明にあっては、チェックポイント関数で起動毎に乱数を生成して課金対象アプリケーションのプログラム識別情報とともに利用記録モジュールへ通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、チェックポイント関数は利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するため、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証することができるとともに、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うことができる。

【００１９】更に、請求項６記載の本発明は、請求項１乃至３のいずれかに記載の本発明において、前記利用記録モジュールが前記課金サーバ装置の公開鍵Ｋｓを保持し、また前記課金サーバ装置は課金サーバ装置自身の私的鍵Ks^{-1}を保持し、前記利用記録モジュールが利用限度を保持し、前記チェックポイント関数の起動回数または単価累積が利用限度に到達すると、乱数R_2を生成し、この生成した乱数R_2と利用記録Ｕを前記課金サーバ装置の公開鍵Ｋｓを用いて暗号化し、この暗号化した情報Ｋｓ（R_2，Ｕ）を前記課金サーバ装置に送信し、前記課金サーバ装置が前記利用記録モジュールから受信した前記暗号化情報Ｋｓ（R_2，Ｕ）を前記課金サーバ装置自身の私的鍵Ks^{-1}を用いて復号して前記乱数R_2と利用記録Ｕを抽出し、前記課金サーバ装置が保持する課金情報を更新し、前記乱数R_2を前記課金サーバ装置自身の私的鍵Ks^{-1}を用いて暗号化し、この暗号化した乱数Ks^{-1}（R_2）を前記利用記録モジュールへ送信し、前記利用記録モジュールが前記課金サーバ装置から受信した前記暗号化乱数Ks^{-1}（R_2）を前記課金サーバ装置の公開鍵Ｋｓを用いて復号し、この復号した乱数R_2’と前記生成した乱数R_2が一致していることを検証し、前記利用記録モジュール内に保持していた利用記録を削除することを要旨とする。

【００２０】請求項６記載の本発明にあっては、利用記

録モジュールから課金サーバ装置へ転送する利用記録および課金サーバ装置から利用記録モジュールへ転送する利用記録受取確認を公開鍵暗号化方式を用いて暗号化し、かつ利用記録および利用記録受取確認に毎回異なる乱数を生成して添付することにより、利用記録が課金サーバ装置へ確実に転送されたことを保証することができる。

【００２１】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００２２】図１は、本発明の一実施形態に関わるプログラムの機能単位利用量課金方法を実施するシステムの構成を示す図である。同図においては、ユーザ処理装置５には予め課金対象機能単位毎にチェックポイント関数１が複数埋め込まれて配布された課金対象アプリケーション７が設けられ、また該課金対象アプリケーション７に隣接して利用記録モジュール２が設けられている。更に、ユーザ処理装置５はネットワークを介して課金サーバ装置３に接続されている。

【００２３】図２は、図１に示すシステムを更に詳しく示したブロック図である。同図に示すように、チェックポイント関数１は、乱数を生成する乱数生成手段１０１、チェックポイント関数１の起動を利用記録モジュール２に通知する起動通知送信手段１０２、利用記録モジュール２から暗号化乱数を受信する暗号化乱数受信手段１０３、暗号化乱数を復号する復号手段１０４、およびこの復号した乱数と前記生成した乱数が一致していることを検証する乱数検出手段１０５を有する。

【００２４】また、利用記録モジュール２は、課金対象アプリケーション７の使用要求を課金サーバ装置３へ送信する使用要求送信手段２０１、課金対象アプリケーション７に対応した暗号鍵を課金サーバ装置３から受信した暗号鍵受信手段２０２、前記暗号鍵を保持する暗号鍵保持手段２０３、チェックポイント関数１からの起動通知を受信する起動通知受信手段２０４、利用記録を管理する記録管理手段２０５、乱数および利用記録を暗号化する暗号化手段２０６、前記暗号化した乱数をチェックポイント関数１へ送信する暗号化乱数送信手段２０７、乱数を生成する乱数生成手段２０８、利用記録を課金サーバ装置３へ送信する利用記録送信手段２０９、課金サーバ装置３から暗号化乱数を受信する暗号化乱数受信手段２１０、前記暗号化乱数を復号する復号手段２１１、および該復号した乱数と前記生成した乱数が一致していることを検証する乱数検証手段２１２を有する。

【００２５】更に、課金サーバ装置３は、課金対象アプリケーション７の使用要求を利用記録モジュール２から受信する使用要求受信手段３０１、課金対象アプリケーション７に対応した暗号鍵を利用記録モジュール２に送信する暗号鍵送信手段３０２、利用記録を利用記録モジュール２から受信する利用記録受信手段３０３、暗号化された乱数および利用記録を復号する復号手段３０４、課金サーバ装置３内部に保持する課金情報を更新する課金情報更新手段３０５、乱数を暗号化する暗号化手段３０６、および暗号化した乱数を利用記録モジュール２に送信する暗号化乱数送信手段３０７を有する。

【００２６】以上のように構成されるプログラムの機能単位利用量課金方法を実施するシステムにおいて、課金対象アプリケーション７の実行に先立ち、前記利用記録モジュール２は、使用要求送信手段２０１が課金対象アプリケーション７のプログラムＩＤを添付してアプリケーション使用要求を前記課金サーバ装置３へ送信する。前記課金サーバ装置３は、使用要求受信手段３０１がプログラムＩＤを添付されたアプリケーション使用要求を前記利用記録モジュール２から受信し、暗号鍵送信手段３０２が前記プログラムＩＤに対応して暗号鍵Ｋを前記利用記録モジュール２へ送信する。前記利用記録モジュール２は、暗号鍵受信手段２０２が前記暗号鍵Ｋを前記課金サーバ装置３から受信し、暗号鍵保持手段２０３が前記暗号鍵Ｋを保持する。

【００２７】課金対象アプリケーションの実行中に、課金対象アプリケーション７の課金対象機能単位毎に埋め込まれた前記チェックポイント関数１が起動されると、前記チェックポイント関数１は、乱数生成手段１０１が乱数R_1を生成し、起動通知送信手段１０２が前記生成した乱数R_1と課金対象アプリケーションのプログラムＩＤと課金対象機能単位の単価とを添付した起動通知を前記利用記録モジュール２へ送信する。

【００２８】前記利用記録モジュール２は、起動通知受信手段２０４が前記乱数R_1と前記プログラムＩＤと前記単価が添付された起動通知を前記チェックポイント関数１から受信し、記録管理手段２０５が前記プログラムＩＤに対応した単価累積を前記単価だけ更新し、暗号化手段２０６が前記暗号鍵保持手段２０３が保持する前記プログラムＩＤに対応した前記暗号鍵Ｋを用いて前記乱数R_1を暗号化し、暗号化乱数送信手段２０７が前記暗号化された乱数Ｋ（R_1）を前記チェックポイント関数１へ送信する。

【００２９】前記チェックポイント関数１は、暗号化乱数受信手段１０３が前記暗号化乱数Ｋ（R_1）を前記利用記録モジュール２から受信し、復号手段１０４がチェックポイント関数１に予め埋め込まれた復号鍵Ｋ’を用いて前記暗号化乱数Ｋ（R_1）を復号し、乱数検証手段１０５が前記復号された乱数R_1’と前記生成した乱数R_1が一致していることを検証する。

【００３０】前記利用記録モジュール２の記録管理手段２０５が保持している単価累積が予め設定されている利用限度に到達すると、前記利用記録モジュール２は、乱数生成手段２０８が乱数R_2を生成し、暗号化手段２０６が利用記録モジュール２内に保持する前記課金サーバ装置３の公開鍵Ｋｓを用いて前記生成した乱数R_2と記

録管理手段２０５が保持している利用記録Ｕとを暗号化し、利用記録送信手段２０９が前記暗号化情報Ｋｓ（R_2，Ｕ）を前記課金サーバ装置３へ送信する。

【００３１】前記課金サーバ装置３は、利用記録受信手段３０３が前記暗号化情報Ｋｓ（R_2，Ｕ）を前記利用記録モジュール２から受信し、復号手段３０４が課金サーバ装置３内に保持する課金サーバ装置自身の秘密鍵Ks^{-1}を用いて前記暗号化情報Ｋｓ（R_2，Ｕ）を復号して前記乱数R_2と前記利用記録Ｕとを抽出し、課金情報更新手段３０５が前記利用記録Ｕを用いて課金情報を更新し、暗号化手段３０６が前記秘密鍵Ks^{-1}を用いて前記乱数R_2を暗号化し、暗号化乱数送信手段３０７が前記暗号化乱数Ks^{-1}（R_2）を前記利用記録モジュール２へ送信する。

【００３２】前記利用記録モジュール２は、暗号化乱数受信手段２１０が前記暗号化乱数Ks^{-1}（R_2）を前記課金サーバ装置３から受信し、復号手段２１１が前記公開鍵Ｋｓを用いて前記暗号化乱数Ks^{-1}（R_2）を復号し、乱数検証手段２１２が前記復号された乱数R_2'と前記生成した乱数R_2が一致していることを検証し、記録管理手段２０５が前記利用記録Ｕを削除する。

【００３３】次に、図３乃至図５に示すフローチャートを参照して、詳細な作用を説明する。

【００３４】図３は、本実施形態において課金対象アプリケーションの実行に先立つ準備段階における処理を示すフローチャートである。利用記録モジュール２は、使用要求送信手段２０１が課金対象アプリケーションのプログラムＩＤを添付したアプリケーション使用要求を課金サーバ装置３へ送信する（ステップＳ１１）。課金サーバ装置３は、使用要求受信手段３０１がプログラムＩＤを添付されたアプリケーション使用要求を利用記録モジュール２から受信し（ステップＳ１３）、暗号鍵送信手段３０２が前記プログラムＩＤに対応した暗号鍵Ｋを利用記録モジュール２へ送信する（ステップＳ１５）。利用記録モジュール２は、暗号鍵受信手段２０２が前記暗号鍵Ｋを課金サーバ装置３から受信し（ステップＳ１７）、暗号鍵保持手段２０３が前記暗号鍵Ｋを保持する（ステップＳ１９）。

【００３５】図４は、本実施形態において課金対象アプリケーションの実行中にチェックポイント関数が起動された時の処理を示すフローチャートである。チェックポイント関数１は、乱数生成手段１０１が乱数R_1を生成し（ステップＳ２１）、起動通知送信手段１０２が前記生成した乱数R_1と課金対象アプリケーションのプログラムＩＤと課金対象機能単位の単価とを添付した起動通知を利用記録モジュール２へ送信する（ステップＳ２３）。

【００３６】利用記録モジュール２は、起動通知受信手段２０４が前記乱数R_1と前記プログラムＩＤと前記単価が添付された起動通知をチェックポイント関数１から受信し（ステップＳ２５）、記録管理手段２０５が前記プログラムＩＤに対応した単価累積を前記単価だけ更新し（ステップＳ２７）、暗号化手段２０６が暗号鍵保持手段２０３が保持する前記プログラムＩＤに対応した前記暗号鍵Ｋを用いて前記乱数R_1を暗号化し（ステップＳ２９）、暗号化乱数送信手段２０７が前記暗号化された乱数Ｋ（R_1）をチェックポイント関数１へ送信する（ステップＳ３１）。

【００３７】チェックポイント関数１は、暗号化乱数受信手段１０３が前記暗号化乱数Ｋ（R_1）を利用記録モジュール２から受信し（ステップＳ３３）、復号手段１０４がチェックポイント関数１に予め埋め込まれた復号鍵Ｋ'を用いて前記暗号化乱数Ｋ（R_1）を復号し（ステップＳ３５）、乱数検証手段１０５が前記復号された乱数R_1'と前記生成した乱数R_1が一致していることを検証する（ステップＳ３７）。

【００３８】図５は、本実施形態において利用記録モジュール２の記録管理手段２０５が保持している単価累積が予め設定されている利用限度に到達した時の処理を示すフローチャートである。利用記録モジュール２は、乱数生成手段２０８が乱数R_2を生成し（ステップＳ４１）、暗号化手段２０６が利用記録モジュール２内に保持する課金サーバ装置３の公開鍵Ｋｓを用いて前記生成した乱数R_2と記録管理手段２０５が保持している利用記録Ｕとを暗号化し（ステップＳ４３）、利用記録送信手段２０９が前記暗号化情報Ｋｓ（R_2，Ｕ）を課金サーバ装置３へ送信する（ステップＳ４５）。

【００３９】課金サーバ装置３は、利用記録受信手段３０３が前記暗号化情報Ｋｓ（R_2，Ｕ）を利用記録モジュール２から受信し（ステップＳ４７）、復号手段３０４が課金サーバ装置３内に保持する課金サーバ装置３自身の秘密鍵Ks^{-1}を用いて前記暗号化情報Ｋｓ（R_2，Ｕ）を復号して前記乱数R_2と前記利用記録Ｕとを抽出し（ステップＳ４９）、課金情報更新手段３０５が前記利用記録Ｕを用いて課金情報を更新し（ステップＳ５１）、暗号化手段３０６が前記秘密鍵Ks^{-1}を用いて前記乱数R_2を暗号化し（ステップＳ５３）、暗号化乱数送信手段３０７が前記暗号化乱数Ks^{-1}（R_2）を利用記録モジュール２へ送信する（ステップＳ５５）。

【００４０】利用記録モジュール２は、暗号化乱数受信手段２１０が前記暗号化乱数Ks^{-1}（R_2）を課金サーバ装置３から受信し（ステップＳ５７）、復号手段２１１が前記公開鍵Ｋｓを用いて前記暗号化乱数Ks^{-1}（R_2）を復号し（ステップＳ５９）、乱数検証手段２１２が前記復号された乱数R_2'と前記生成した乱数R_2が一致していることを検証し（ステップＳ６１）、記録管理手段２０５が前記利用記録Ｕを削除する（ステップＳ６３）。

【００４１】

【発明の効果】以上説明したように、本発明によれば、

課金対象アプリケーション内に課金対象機能単位毎に予め埋め込まれているチェックポイント関数は起動される毎に起動通知を利用記録モジュールへ通知し、利用記録モジュールは起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するので、課金対象機能単位毎に実行回数に応じた課金が可能である。

【００４２】また、本発明によれば、チェックポイント関数は起動される毎に課金対象アプリケーションのプログラム識別情報を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、この利用記録を課金サーバ装置に転送するので、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うことができる。

【００４３】更に、本発明によれば、チェックポイント関数は起動される毎に単価を添付した起動通知を利用記録モジュールに通知し、利用記録モジュールは単価の累積を更新し、この利用記録を課金サーバ装置に転送するため、課金対象機能単位毎に単価を設定して、課金対象機能単位の開発工数、規模、ノウハウ、難易度、利用価値などにより課金対象機能単位毎に異なる料金を徴収することができる。

【００４４】本発明によれば、チェックポイント関数で起動毎に乱数を生成して利用記録モジュールへ通知し、利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するので、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証することができる。

【００４５】また、本発明にあっては、チェックポイント関数で起動毎に乱数を生成して課金対象アプリケーションのプログラム識別情報とともに利用記録モジュールへ通知し、利用記録モジュールはプログラム識別情報毎に起動通知の回数を更新し、チェックポイント関数は利用記録モジュールから返却された暗号化乱数を復号して元の乱数と比較検証するので、課金対象機能単位の実行回数に応じた利用記録が取得されることを保証することができるとともに、プログラム識別情報を用いて課金対象アプリケーション毎に利用記録を集計することにより、課金対象機能単位の実行回数に応じて課金対象アプリケーションの権利保持者への利用料金支払いを行うことができる。

【００４６】更に、本発明によれば、利用記録モジュールから課金サーバ装置へ転送する利用記録および課金サーバ装置から利用記録モジュールへ転送する利用記録受取確認を公開鍵暗号化方式を用いて暗号化し、かつ利用記録および利用記録受取確認に毎回異なる乱数を生成して添付するので、利用記録が課金サーバ装置へ確実に転送されたことを保証することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係わるプログラムの機能単位利用量課金方法を実施するシステムの構成を示す図である。

【図２】図１に示すシステムを更に詳しく示したブロック図である。

【図３】図１に示す実施形態において課金対象アプリケーションの実行に先立つ準備段階における処理を示すフローチャートである。

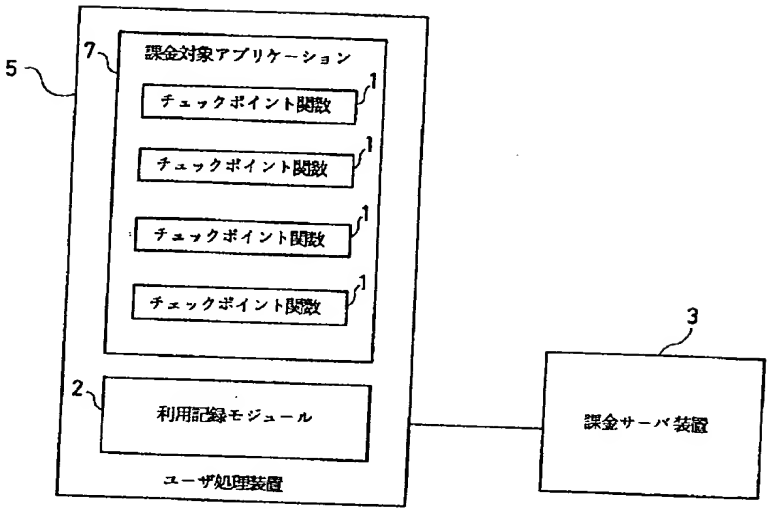
【図４】図１に示す実施形態において課金対象アプリケーションの実行中にチェックポイント関数が起動された時の処理を示すフローチャートである。

【図５】図１に示す実施形態において利用記録モジュールの記録管理手段が保持している単価蓄積が予め設定されている利用限度に到達した時の処理を示すフローチャートである。

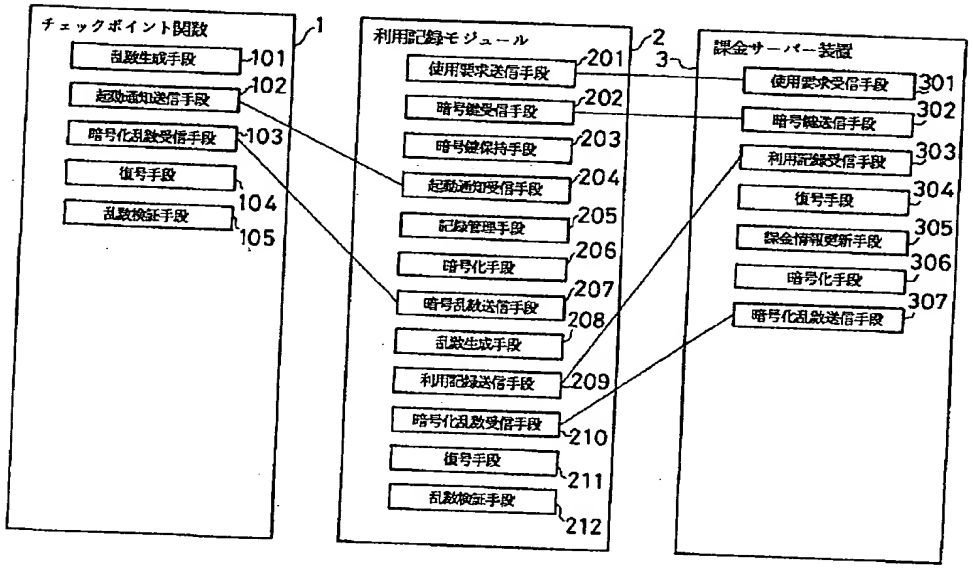
【符号の説明】

１　チェックポイント関数
２　利用記録モジュール
３　課金サーバ装置
５　ユーザ処理装置
７　課金対象アプリケーション
１０１　乱数生成手段
１０２　起動通知送信手段
１０５　乱数検証手段
２０１　使用要求送信手段
２０２　暗号鍵受信手段
２０４　起動通知受信手段
２０５　記録管理手段
２０９　利用記録送信手段
２１２　乱数検証手段
３０１　使用要求受信手段
３０２　暗号鍵送信手段
３０７　暗号化乱数送信手段

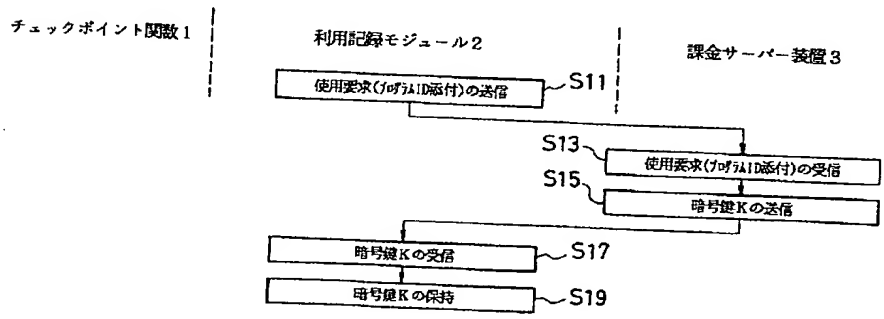
【図１】


5
7
課金対象アプリケーション
チェックポイント関数
1
チェックポイント関数
1
チェックポイント関数
1
チェックポイント関数
1
2
利用記録モジュール
ユーザ処理装置
3
課金サーバ装置

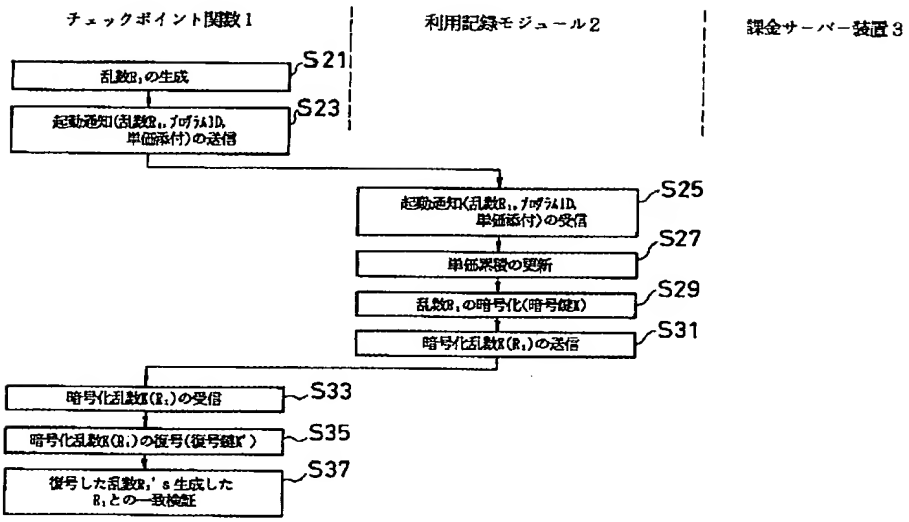
【図２】


チェックポイント関数
1
乱数生成手段
101
起動通知送信手段
102
暗号化乱数受信手段
103
復号手段
104
乱数検証手段
105
利用記録モジュール
2
使用要求送信手段
201
暗号鍵受信手段
202
暗号鍵保持手段
203
起動通知受信手段
204
記録管理手段
205
暗号化手段
206
暗号乱数送信手段
207
乱数生成手段
208
利用記録送信手段
209
暗号化乱数受信手段
210
復号手段
211
乱数検証手段
212
課金サーバー装置
3
使用要求受信手段
301
暗号鍵送信手段
302
利用記録受信手段
303
復号手段
304
課金情報更新手段
305
暗号化手段
306
暗号化乱数送信手段
307

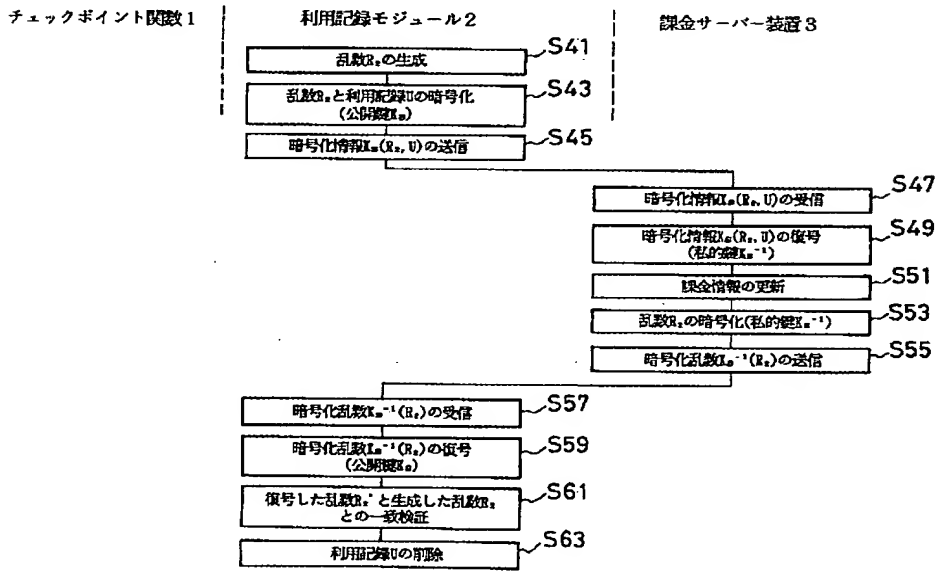
【図３】


チェックポイント関数1
利用記録モジュール2
課金サーバー装置3
使用要求(プログラムID添付)の送信
S11
S13
使用要求(プログラムID添付)の受信
S15
暗号鍵Kの送信
暗号鍵Kの受信
S17
暗号鍵Kの保持
S19

【図４】


チェックポイント関数１
利用記録モジュール２
課金サーバー装置３
乱数R1の生成
S21
起動通知(乱数R1,プログラムID,単価添付)の送信
S23
起動通知(乱数R1,プログラムID,単価添付)の受信
S25
単価累算の更新
S27
乱数R1の暗号化(暗号鍵K)
S29
暗号化乱数X(R1)の送信
S31
暗号化乱数X(R1)の受信
S33
暗号化乱数X(R1)の復号(復号鍵K')
S35
復号した乱数R1'とR1との一致検証
S37

【図５】


チェックポイント関数１
利用記録モジュール２
課金サーバー装置３
乱数Rsの生成
S41
乱数Rsと利用記録Uの暗号化(公開鍵Ks)
S43
暗号化情報Ks(Rs,U)の送信
S45
暗号化情報Ks(Rs,U)の受信
S47
暗号化情報Ks(Rs,U)の復号(私的鍵Ks-1)
S49
課金情報の更新
S51
乱数R1の暗号化(私的鍵K-1)
S53
暗号化乱数K-1(R1)の送信
S55
暗号化乱数K-1(R1)の受信
S57
暗号化乱数Ks-1(Rs)の復号(公開鍵Ks)
S59
復号した乱数Rs'と生成した乱数Rsとの一致検証
S61
利用記録Uの削除
S63

Japanese Patent Application Laid-Open No. 11-53185

Date of Laid-Open: February 26, 1999

[Title of the Invention]

METHOD OF CHARGING FOR PROGRAM ON THE BASIS OF AMOUNT OF USE OF EACH FUNCTION UNIT

[Abstract]

[Objective] To provide a method of charging for a program on the basis of amount of use of each function unit, which method enables collection of a usage fee which is charged for each function of software in proportion to the number of times the function has been used.

[Means for Solution] Before execution of a chargeable application, a usage recording module 2 transmits an application usage request to a charging server apparatus 3. The charging server apparatus 3 transmits an encryption key K to the usage recording module 2. During execution of the chargeable application, a check point function 1 generates a random number R_1, and transmits to the usage recording module an activation report to which is attached the random number, whenever the check point function 1 is activated. The usage recording module updates the number of the activation reports, encrypts, by making use of the encryption key K, the random number R_1 received from the check point function, and returns the encrypted random number to the check point function. The check point function decrypts, by making use of a decryption key K', the encrypted random number $K(R_1)$ received from the

usage recording module, and verifies whether the random number R_1' coincides with the random number R_1.

[Claims]

[Claim 1] A method of charging for a program on the basis of amount of use of each function unit, the method being adapted for a program charging system which includes a usage recording module provided in a user processing apparatus having a chargeable application, and a charging server apparatus which is connected to the user processing apparatus via a network, and being characterized in that

the chargeable application is distributed in a state in which a check point function is previously embedded for each chargeable function unit;

the check point function transmits an activation report to the usage recording module whenever activated; and

the usage recording module updates and holds the number of the activation reports and transfers the held usage record to the charging server apparatus.

[Claim 2] A method of charging for a program on the basis of amount of use of each function unit, described in claim 1 and characterized in that

the check point function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by program identification information of the chargeable application; and

the usage recording module updates and holds the number of the activation reports for each piece of program

identification information, and transmits the held usage record to the charging server apparatus.

[Claim 3] A method of charging for a program on the basis of amount of use of each function unit, described in claim 1 or 2 and characterized in that

the check point function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by a unit price; and

the usage recording module updates and holds the cumulative unit prices, and transmits the held usage record to the charging server apparatus.

[Claim 4] A method of charging for a program on the basis of amount of use of each function unit, described in any one of claims 1 to 3 and characterized in that

a decryption key K' is embedded in the check point function in advance;

before execution of the chargeable application, the usage recording module transmits an application usage request to the charging server apparatus;

the charging server apparatus transmits to the usage recording module an encryption key K corresponding to the decryption key K';

the usage recording module holds the encryption key K received from the charging server apparatus;

during execution of the chargeable application, the check point function generates a random number R_1 and transmits to the usage recording module an activation report

to which is attached the generated random number R_1, whenever the check point function is activated;

the usage recording module updates and holds the number of the activation reports, encrypts, by making use of the encryption key K, the random number R_1 received from the check point function, and returns the encrypted random number $K(R_1)$ to the check point function;

the check point function decrypts, by making use of the decryption key K', the encrypted random number $K(R_1)$ received from the usage recording module, and verifies whether the decrypted random number R_1' coincides with the generated random number R_1'; and

the usage recording module transmits the usage record held therein to the charging server apparatus.

[Claim 5] A method of charging for a program on the basis of amount of use of each function unit, described in any one of claims 1 to 3 and characterized in that

a decryption key K' is embedded in the check point function in advance;

before execution of the chargeable application, the usage recording module transmits to the charging server apparatus an application usage request accompanied by program identification information of the chargeable application;

the charging server apparatus transmits to the usage recording module an encryption key K corresponding to the decryption key K' embedded in the chargeable application designated by the program identification information;

the usage recording module holds the encryption key K received from the charging server apparatus in such a manner that the encryption key K is paired with the program identification information;

during execution of the chargeable application, the check point function generates a random number R_1 and transmits to the usage recording module an activation report to which are attached the generated random number R_1 and the program identification information of the chargeable application, whenever the check point function is activated;

the usage recording module updates and holds the number of activation reports for each piece of program identification information, encrypts, by making use of the encryption key K corresponding to the program identification information, the random number R_1 received from the check point function, and returns the encrypted random number $K(R_1)$ to the check point function;

the check point function decrypts, by making use of a decryption key K', the encrypted random number $K(R_1)$ received from the usage recording module, and verifies whether the decrypted random number R_1' coincides with the generated random number R_1; and

the usage recording module transmits the usage record held therein to the charging server apparatus.

[Claim 6] A method of charging for a program on the basis of amount of use of each function unit, described in any one of claims 1 to 3 and characterized in that

the usage recording module holds a public key Ks of the charging server apparatus, the charging server apparatus holds a private key Ks^{-1} of the charging server apparatus itself;

the usage recording module holds a usable limit, and when the number of times of activation or the cumulative unit prices of the check point function reaches the usable limit, the usage recording module generates a random number R_2, encrypts the generated random number R_2 and a usage record U by making use of the public key Ks of the charging server apparatus, and transmits the encrypted information Ks (R_2, U) to the charging server apparatus;

the charging server apparatus decrypts the encrypted information Ks (R_2, U) received from the usage recording module by making use of the private key Ks^{-1} of the charging server apparatus itself to thereby extract the random number R_2 and the usage record U, updates charge information held in the charging server apparatus, encrypts the random number R_2 by making use of the private key Ks^{-1} of the charging server apparatus itself, transmits the encrypted random number $Ks^{-1}(R_2)$ to the usage recording module; and

the usage recording module decrypts, by making use of the public key Ks of the charging server apparatus, the encrypted random number $Ks^{-1}(R_2)$ received from the charging server apparatus, verifies whether the decrypted random number R_2' coincides with the generated random number R_2, and deletes the usage record held in the usage recording module.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] The present invention relates to a method of charging, on the basis of amount of use of each function unit, for software that is distributed while being stored in a medium such as a CD-ROM or a floppy disk, or software that is distributed via a network.

[0002]

[Prior Art] A conventional software charging system employs a method of charging for a program such that software is sold, and the charging is ended when a user purchases the software.

[0003] In another existing charging system, when a user uses distributed software, the user notifies a charging center of the use of the software, on the basis of which the charging center charges for use of the software.

[0004] Further, recently, a buying-out scheme has been adopted. In this scheme, encrypted software is distributed by use of a medium such as a CD-ROM or via a network, and after completion of a purchase procedure performed by phone, facsimile, letter, or electronic mail, a decryption key is provided. Further, there have been other methods, such as a method in which software which has been encrypted and for which an usable amount has been set is distributed, the number of days over which a user uses the software is managed as an amount of use, and charging is effected on the basis of the number of days.

[0005]

[Problems to be Solved by the Invention] However, when the above-described buying-out scheme is employed, a large number of functions are incorporated in software in order to reduce distribution cost to a relatively low level, and a user must pay a large amount of money for functions that the user hardly uses. Further, the user cannot judge whether the software provides a necessary function unless the user purchases and executes the software.

[0006] Further, sole use of the method in which, before use of distributed software, a user notifies a charging center of the use of the software raises a problem in that the method cannot cope with unpaid usage fees, because the method cannot restrict use of the software, although it can charge for use of the software.

[0007] The system in which encrypted software is distributed in advance and a decryption key is provided before use of the software has a drawback in that, since a user must pay a fixed amount of money regardless of the number of times of use, price per time of use or per unit time of use varies greatly among users.

[0008] The present invention was accomplished in view of the foregoing, and an object of the present invention is to provide a method of charging for a program on the basis of amount of use of each function unit, which method enables collection of a usage fee which is charged for each function of software in proportion to the number of times the function has been used.

[0009]

[Means to Solve the Problems] In order to achieve the above object, the invention described in claim 1 is directed to a program charging system which includes a usage recording module provided in a user processing apparatus having a chargeable application, and a charging server apparatus which is connected to the user processing apparatus via a network, characterized in that the chargeable application is distributed in a state in which a check point function is previously embedded for each chargeable function unit; the check point function transmits an activation report to the usage recording module whenever activated; and the usage recording module updates and holds the number of the activation reports and transfers the held usage record to the charging server apparatus.

[0010] In the invention described in claim 1, whenever the check point function which is previously embedded in a chargeable application for each chargeable function unit is activated, the check point function transmits an activation report to the usage recording module; and the usage recording module updates the number of the activation reports and transfers the held usage record to the charging server apparatus. Therefore, it is possible to charge for each chargeable function unit in accordance with the number of times of execution of the chargeable function unit.

[0011] The invention described in claim 2 is characterized in that, in the invention of claim 1, the check point

function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by program identification information of the chargeable application; and the usage recording module updates and holds the number of the activation reports for each piece of program identification information, and transmits the held usage record to the charging server apparatus.

[0012] In the invention described in claim 2, the check point function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by program identification information of the chargeable application; and the usage recording module updates the number of the activation reports for each piece of program identification information, and transmits this usage record to the charging server apparatus. Therefore, it is possible for the user to pay usage fee to the proprietor of the chargeable application in accordance with the number of times of execution of the chargeable function unit, through summing up usage records for each chargeable application by use of the program identification information.

[0013] The invention described in claim 3 is characterized in that, in the invention of claim 1 or 2, the check point function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by a unit price; and the usage recording module updates and holds the cumulative unit prices, and

transmits the held usage record to the charging server apparatus.

[0014] In the invention described in claim 3, the check point function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by a unit price; and the usage recording module updates the cumulative unit prices, and transmits this usage record to the charging server apparatus. Therefore, it is possible to collect a different fee for use of each different chargeable function unit, depending on man-hours and know-how needed for developing the function unit, the scale, difficulty, and utility of the function unit, through setting of a unit price for each different chargeable function unit.

[0015] The invention described in claim 4 is characterized in that, in the invention of any one of claims 1 to 3, a decryption key K' is embedded in the check point function in advance; before execution of the chargeable application, the usage recording module transmits an application usage request to the charging server apparatus; the charging server apparatus transmits to the usage recording module an encryption key K corresponding to the decryption key K'; the usage recording module holds the encryption key K received from the charging server apparatus; during execution of the chargeable application, the check point function generates a random number R_1 and transmits to the usage recording module an activation report to which is attached the generated

random number R_1, whenever the check point function is activated; the usage recording module updates and holds the number of the activation reports, encrypts, by making use of the encryption key K, the random number R_1 received from the check point function, and returns the encrypted random number $K(R_1)$ to the check point function; the check point function decrypts, by making use of the decryption key K', the encrypted random number $K(R_1)$ received from the usage recording module, and verifies whether the decrypted random number R_1' coincides with the generated random number R_1'; and the usage recording module transmits the usage record held therein to the charging server apparatus.

[0016] In the invention described in claim 4, whenever the check point function is activated, the check point function generates a random number and transmits it to the usage recording module, decrypts the encrypted random number returned from the usage recording module, and compares it with the original random number for verification. Therefore, it is possible to guarantee that a usage record corresponding to the number of times of execution of the chargeable function unit can be obtained.

[0017] The invention described in claim 5 is characterized in that, in the invention of any one of claims 1 to 3, a decryption key K' is embedded in the check point function in advance; before execution of the chargeable application, the usage recording module transmits to the charging server apparatus an application usage request accompanied by program

identification information of the chargeable application; the charging server apparatus transmits to the usage recording module an encryption key K corresponding to the decryption key K' embedded in the chargeable application designated by the program identification information; the usage recording module holds the encryption key K received from the charging server apparatus in such a manner that the encryption key K is paired with the program identification information; during execution of the chargeable application, the check point function generates a random number R_1 and transmits to the usage recording module an activation report to which are attached the generated random number R_1 and the program identification information of the chargeable application, whenever the check point function is activated; the usage recording module updates and holds the number of activation reports for each piece of program identification information, encrypts, by making use of the encryption key K corresponding to the program identification information, the random number R_1 received from the check point function, and returns the encrypted random number $K(R_1)$ to the check point function; the check point function decrypts, by making use of a decryption key K', the encrypted random number $K(R_1)$ received from the usage recording module, and verifies whether the decrypted random number R_1' coincides with the generated random number R_1; and the usage recording module transmits the usage record held therein to the charging server apparatus.

[0018] In the invention described in claim 5, whenever the check point function is activated, the check point function generates a random number and transmits it to the usage recording module together with program identification information; the usage recording module updates the number of activation reports for each piece of program identification information; and the check point function decrypts the encrypted random number returned from the usage recording module, and compares it with the original random number for verification. Therefore, it is possible to guarantee that a usage record corresponding to the number of times of execution of the chargeable function unit can be obtained. Further, it becomes possible for the user to pay a usage fee to the proprietor of the chargeable application in accordance with the number of times of execution of the chargeable function unit, through summing up of usage records for each chargeable application by use of the of program identification information.

[0019] The invention described in claim 6 is characterized in that, in the invention of any one of claims 1 to 3, the usage recording module holds a public key Ks of the charging server apparatus, the charging server apparatus holds a private key Ks^{-1} of the charging server apparatus itself; and the usage recording module holds a usable limit, and when the number of times of activation or the cumulative unit prices of the check point function reaches the usable limit, the usage recording module generates a random number R_2, encrypts

the generated random number R_2 and a usage record U by making use of the public key Ks of the charging server apparatus, and transmits the encrypted information Ks (R_2, U) to the charging server apparatus; the charging server apparatus decrypts the encrypted information Ks (R_2, U) received from the usage recording module by making use of the private key Ks^{-1} of the charging server apparatus itself to thereby extract the random number R_2 and the usage record U, updates charge information held in the charging server apparatus, encrypts the random number R_2 by making use of the private key Ks^{-1} of the charging server apparatus itself, transmits the encrypted random number $Ks^{-1}(R_2)$ to the usage recording module; and the usage recording module decrypts, by making use of the public key Ks of the charging server apparatus, the encrypted random number $Ks^{-1}(R_2)$ received from the charging server apparatus, verifies whether the decrypted random number R_2' coincides with the generated random number R_2, and deletes the usage record held in the usage recording module.

[0020] In the invention described in claim 6, a usage record transmitted from the usage recording module to the charging server apparatus and a usage-record receipt acknowledgement transmitted from the charging server apparatus to the usage recording module are encrypted by use of a public-key cryptosystem, and, for each time, a different random number is generated and attached to the usage record and the usage-record receipt acknowledgment. Therefore, it becomes

possible to guarantee that the usage record has been transferred to the charging server apparatus without fail.

[0021]

[Embodiment of the Invention] Hereinbelow, an embodiment of the present invention will be described with reference to the drawings.

[0022] FIG. 1 is a diagram showing the configuration of a system which implements the method of charging for a program on the basis of amount of use of each function unit, according to the embodiment of the present invention. As shown in FIG. 1, a distributed application 7 to be charged (chargeable application) is provided in a user processing apparatus 5. A plurality of check point functions 1 are embedded in the chargeable application 7 in advance such that one check point function 1 is provided for each function unit to be charged (chargeable function unit). In addition, a usage recording module 2 is provided adjacent to the chargeable application 7. Moreover, a charging server apparatus 3 is connected to the user processing apparatus 5 via a network.

[0023] FIG. 2 shows a block diagram showing the system of FIG. 1 in more detail. As shown in FIG. 2, the check point function 1 includes random-number generation means 101 for generating a random number; activation-report transmission means 102 for reporting activation of the check point function 1 to the usage recording module 2; encrypted-random-number reception means 103 for receiving an encrypted random

number from the usage recording module 2; decryption means 104 for decrypting the encrypted random number; and random-number detection means 105 for checking whether the decrypted random number coincides with the above-described generated random number.

[0024] The usage recording module 2 includes usage-request transmission means 201 for transmitting to the charging server apparatus 3 a request for using the chargeable application 7; encryption-key reception means 202 for receiving from the charging server apparatus 3 an encryption key corresponding to the chargeable application 7; encryption-key holding means 203 for holding the encryption key; activation-report reception means 204 for receiving an activation report from the check point function 1; record management means 205 for managing a usage record; encryption means 206 for encrypting a random number and the usage record; encrypted-random-number transmission means 207 for transmitting the encrypted random number to the check point function 1; random-number generation means 208 for generating the random number; usage-record transmission means 209 for transmitting the usage record to the charge server apparatus 3; encrypted-random-number reception means 210 for receiving an encrypted random number from the charge server apparatus 3; decryption means 211 for decrypting the encrypted random number; and random-number verification means 212 for verifying whether the decrypted random number coincides with the above-described generated random number.

[0025] The charging server apparatus 3 includes usage-request reception means 301 for receiving from the usage recording module 2 the request for using the chargeable application 7; encryption-key transmission means 302 for transmitting to the usage recording module 2 an encryption key corresponding to the chargeable application 7; usage-record reception means 303 for receiving the usage record from the usage recording module 2; decryption means 304 for decrypting the encrypted random number and usage record; charging-information update means 305 for updating charging information held in the charging server apparatus 3; encryption means 306 for encrypting a random number; and encrypted-random-number transmission means 307 for transmitting the encrypted random number to the usage recording module 2.

[0026] In the system which has the above-described configuration and which implements the method of charging for a program on the basis of amount of use of each function unit, before execution of the chargeable application 7, the usage-request transmission means 201 in the usage recording module 2 transmits an application usage request to the charging server apparatus 3 together with a program ID of the chargeable application 7. In the charging server apparatus 3, the usage-request reception means 301 receives from the usage recording module 2 the application usage request accompanied by the program ID; and the encryption-key transmission means 302 transmits to the usage recording module 2 an encryption

key K corresponding to the program ID. In the usage recording module 2, the encryption-key reception means 202 receives the encryption key K from the charging server apparatus 3; and the encryption-key holding means 203 holds the encryption key K.

[0027] When the check point function 1——which is embedded in the chargeable application 7 for each chargeable function——is activated during execution of the chargeable application 7, within the check point function 1 the random-number generation means 101 generates a random number R_1; and the activation-report transmission means 102 transmits to the usage recording module 2 an activation report to which is attached the generated random number R_1, the program ID of the chargeable application 7, and a unit price of the chargeable function unit.

[0028] In the usage recording module 2, the activation-report reception means 204 receives from the check point function 1 the activation report accompanied by the generated random number R_1, the program ID, and the unit price; the record management means 205 updates the cumulative unit prices corresponding to the program ID by the unit price; the encryption means 206 encrypts the random number R_1, by making use of the encryption key K corresponding to the program ID held in the encryption-key holding means 203; and the encrypted-random-number transmission means 207 transmits the encrypted random number $K(R_1)$ to the check point function 1.

[0029] In the check point function 1, the encrypted-random-

number reception means 103 receives the encrypted random number $K(R_1)$ from the usage recording module 2; the decryption means 104 decrypts the encrypted random number $K(R_1)$ by making use of a decryption key K' which has been embedded in the check point function 1 in advance; and the random-number verification means 105 verifies whether the decrypted random number R_1' coincides with the generated random number R_1.

[0030] When the cumulative unit prices held in the record management means 205 of the usage recording module 2 reach a preset usable limit, in the usage recording module 2 the random-number generation means 208 generates a random number R_2; the encryption means 206 encrypts the generated random number R_2 and a usage record U held in the record management means 205, by making use of a public key Ks of the charging server apparatus 3 held in the usage recording module 2; and the usage-record transmission means 209 transmits the encrypted information Ks (R_2, U) to the charging server apparatus 3.

[0031] In the charging server apparatus 3, the usage-record reception means 303 receives the encrypted information Ks (R_2, U) from the usage recording module 2; the decryption means 304 decrypts the encrypted information Ks (R_2, U) by making use of a private key Ks^{-1} of the charging server apparatus 3 held therein to thereby extract the random number R_2 and the usage record U; the charging-information update means 305 updates the charge information on the basis of the usage

record U; the encryption means 306 encrypts the random number R_2 by making use of the private key Ks^{-1}; and the encrypted-random-number transmission means 307 transmits the encrypted random number $Ks^{-1}(R_2)$ to the usage recording module 2.

[0032] In the usage recording module 2, the encrypted-random-number reception means 210 receives the encrypted random number $Ks^{-1}(R_2)$ from the charging server apparatus 3; the decryption means 211 decrypts the encrypted random number $Ks^{-1}(R_2)$ by making use of the public key Ks; the random-number verification means 212 verifies whether the decrypted random number R_2' coincides with the generated random number R_2; and the record management means 205 deletes the usage record U.

[0033] Next, the operation will be described in detail with reference to the flowcharts shown in FIGS. 3 to 5.

[0034] FIG. 3 is a flowchart showing processing performed in a preparation stage preceding to execution of a chargeable application in the present embodiment. In the usage recording module 2, the usage-request transmission means 201 transmits an application usage request to the charging server apparatus 3 together with the program ID of the chargeable application (step S11). In the charging server apparatus 3, the usage-request reception means 301 receives from the usage recording module 2 the application usage request accompanied by the program ID (step S13); and the encryption-key transmission means 302 transmits to the usage recording module 2 an encryption key corresponding to the program ID (step S15). In the usage recording module 2, the encryption-

key reception means 202 receives the encryption key K from the charging server apparatus 3 (step S17); and the encryption-key holding means 203 holds the encryption key K (step S19).

[0035] FIG. 4 is a flowchart showing processing performed when a check point function is activated during execution of the chargeable application in the present embodiment. In the check point function 1, the random-number generation means 101 generates a random number R_1 (step S21); and the activation-report transmission means 102 transmits to the usage recording module 2 an activation report to which is attached the generated random number R_1, the program ID of the chargeable application 7, and a unit price of the chargeable function unit (step S23).

[0036] In the usage recording module 2, the activation-report reception means 204 receives from the check point function 1 the activation report accompanied by the random number R_1, the program ID, and the unit price (step S25); the record management means 205 updates the cumulative unit prices corresponding to the program ID by the unit price (step S27); the encryption means 206 encrypts the random number R_1, by making use of the encryption key K corresponding to the program ID held in the encryption-key holding means 203 (step S29); and the encrypted-random-number transmission means 207 transmits the encrypted random number $K(R_1)$ to the check point function 1 (step S31).

[0037] In the check point function 1, the encrypted-random-

number reception means 103 receives the encrypted random number $K(R_1)$ from the usage recording module 2 (step S33); the decryption means 104 decrypts the encrypted random number $K(R_1)$ by making use of a decryption key K' which has been embedded in the check point function 1 in advance (step s35); and the random-number verification means 105 verifies whether the decrypted random number R_1' coincides with the generated random number R_1 (step S37).

[0038] FIG. 5 is a flowchart showing processing performed when the cumulative unit prices held in the record management means 205 of the usage recording module 2 reach the preset usable limit in the present embodiment. In the usage recording module 2, the random-number generation means 208 generates a random number R_2 (step S41); the encryption means 206 encrypts the generated random number R_2 and a usage record U held in the record management means 205, by making use of a public key Ks of the charging server apparatus 3 held in the usage recording module 2 (step S43); and the usage-record transmission means 209 transmits the encrypted information Ks (R_2, U) to the charging server apparatus 3 (step S45).

[0039] In the charging server apparatus 3, the usage-record reception means 303 receives the encrypted information Ks (R_2, U) from the usage recording module 2 (step S47); the decryption means 304 decrypts the encrypted information Ks (R_2, U) by making use of a private key Ks^{-1} of the charging server apparatus 3 held therein to thereby extract the random

number R_2 and the usage record U (step S49); the charging-information update means 305 updates the charge information on the basis of the usage record U (step S51); and the encryption means 306 encrypts the random number R_2 by making use of the private key Ks^{-1} (step S53); and the encrypted-random-number transmission means 307 transmits the encrypted random number $Ks^{-1}(R_2)$ to the usage recording module 2 (step S55).

[0040] In the usage recording module 2, the encrypted-random-number reception means 210 receives the encrypted random number $Ks^{-1}(R_2)$ from the charging server apparatus 3 (step S57); the decryption means 211 decrypts the encrypted random number $Ks^{-1}(R_2)$ by making use of the public key Ks (step S59); the random-number verification means 212 verifies whether the decrypted random number R_2' coincides with the generated random number R_2 (step S61); and the record management means 205 deletes the usage record U (step S63).

[0041]

[Effects of the Invention]

As described above, according to the present invention, whenever the check point function which is previously embedded in a chargeable application for each chargeable function unit is activated, the check point function transmits an activation report to the usage recording module; and the usage recording module updates the number of the activation reports and transfers this usage record to the charging server apparatus. Therefore, it is possible to

charge for each chargeable function unit in accordance with the number of times of execution of the chargeable function unit.

[0042] Further, according to the present invention, the check point function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by program identification information of the chargeable application; and the usage recording module updates the number of the activation reports for each piece of program identification information, and transmits this usage record to the charging server apparatus. Therefore it is possible for the user to pay usage fee to the proprietor of the chargeable application in accordance with the number of times of execution of the chargeable function unit, through summing up usage records for each chargeable application by use of the program identification information.

[0043] Further, according to the present invention, the check point function transmits to the usage recording module an activation report whenever activated, the activation report being accompanied by a unit price; and the usage recording module updates the cumulative unit prices, and transmits this usage record to the charging server apparatus. Therefore, it is possible to collect a different fee for use of each different chargeable function unit, depending on man-hours and know-how needed for developing the function unit, the scale, difficulty, and utility of the function unit, through setting of a unit price for each different chargeable

function unit.

[0044] Further, according to the present invention, whenever the check point function is activated, the check point function generates a random number and transmits it to the usage recording module, decrypts the encrypted random number returned from the usage recording module, and compares it with the original random number for verification. Therefore, it is possible to guarantee that a usage record corresponding to the number of times of execution of the chargeable function unit can be obtained.

[0045] Further, according to the present invention, whenever the check point function is activated, the check point function generates a random number and transmits it to the usage recording module together with program identification information of the chargeable application; the usage recording module updates the number of activation reports for each piece of program identification information; and the check point function decrypts the encrypted random number returned from the usage recording module, and compares it with the original random number for verification. Therefore, it is possible to guarantee that a usage record corresponding to the number of times of execution of the chargeable function unit can be obtained. Further, it becomes possible for the user to pay a usage fee to the proprietor of the chargeable application in accordance with the number of times of execution of the chargeable function unit, through summing up of usage records for each chargeable application by use of

the of program identification information.

[0046] Further, according to the present invention, a usage record transmitted from the usage recording module to the charging server apparatus and a usage-record receipt acknowledgement transmitted from the charging server apparatus to the usage recording module are encrypted by use of a public-key cryptosystem, and, for each time, a different random number is generated and attached to the usage record and the usage-record receipt acknowledgment. Therefore, it becomes possible to guarantee that the usage record has been transferred to the charging server apparatus without fail.

[Brief Description of the Drawings]

[FIG. 1] Diagram showing the configuration of a system which implements the method of charging for a program on the basis of amount of use of each function unit, according to the embodiment of the present invention.

[FIG. 2] Block diagram showing the system of FIG. 1 in more detail.

[FIG. 3] Flowchart showing processing performed in a preparation stage preceding to execution of a chargeable application in the embodiment shown in FIG. 1.

[FIG. 4] Flowchart showing processing performed when a check point function is activated during execution of the chargeable application in the embodiment shown in FIG. 1.

[FIG. 5] Flowchart showing processing performed when the cumulative unit prices held in the record management means of the usage recording module reaches the preset usable limit in

the embodiment shown in FIG. 1.

[Description of Reference Numerals]

1: check point function

2: usage recording module

3: charging server apparatus

5: user processing apparatus

7: chargeable application

101: random-number generation means

102: activation-report transmission means

105: random-number verification means

201: usage-request transmission means

202: encryption-key reception means

204: activation-report reception means

205: record management means

209: usage-record transmission means

212: random-number verification means

301: usage-request reception means

302: encryption-key transmission means

307: encrypted-random-number transmission means

FIG. 1

1: CHECK POINT FUNCTION

2: USAGE RECORDING MODULE

3: CHARGING SERVER APPARATUS

5: USER PROCESSING APPARATUS

7: CHARGEABLE APPLICATION

FIG. 2

1: CHECK POINT FUNCTION

2: USAGE RECORDING MODULE

3: CHARGING SERVER APPARATUS

101: RANDOM-NUMBER GENERATION MEANS

102: ACTIVATION-REPORT TRANSMISSION MEANS

103: ENCRYPTED-RANDOM-NUMBER RECEPTION MEANS

104: DECRYPTION MEANS

105: RANDOM-NUMBER VERIFICATION MEANS

201: USAGE-REQUEST TRANSMISSION MEANS

202: ENCRYPTION-KEY RECEPTION MEANS

203: ENCRYPTION-KEY HOLDING MEANS

204: ACTIVATION-REPORT RECEPTION MEANS

205: RECORD MANAGEMENT MEANS

206: ENCRYPTION MEANS

207: ENCRYPTED-RANDOM-NUMBER TRANSMISSION MEANS

208: RANDOM-NUMBER GENERATION MEANS

209: USAGE-RECORD TRANSMISSION MEANS

210: ENCRYPTED-RANDOM-NUMBER RECEPTION MEANS

211: DECRYPTION MEANS

212: RANDOM-NUMBER VERIFICATION MEANS

301: USAGE-REQUEST RECEPTION MEANS

302: ENCRYPTION-KEY TRANSMISSION MEANS

303: USAGE-RECORD RECEPTION MEANS

304: DECRYPTION MEANS

305: CHARGING-INFORMATION UPDATE MEANS

306: ENCRYPTION MEANS

307: ENCRYPTED-RANDOM-NUMBER TRANSMISSION MEANS

FIG. 3

1: CHECK POINT FUNCTION

2: USAGE RECORDING MODULE

3: CHARGING SERVER APPARATUS

S11: TRANSMIT USAGE REQUEST (PROGRAM ID ATTACHED)

S13: RECEIVE USAGE REQUEST (PROGRAM ID ATTACHED)

S15: TRANSMIT ENCRYPTION KEY K

S17: RECEIVE ENCRYPTION KEY K

S19: HOLD ENCRYPTION KEY K

FIG. 4

1: CHECK POINT FUNCTION

2: USAGE RECORDING MODULE

3: CHARGING SERVER APPARATUS

S21: GENERATE RANDOM NUMBER R_1

S23: TRANSMIT ACTIVATION REPORT (RANDOM NUMBER R_1, PROGRAM ID, AND UNIT PRICE ATTACHED)

S25: RECEIVE ACTIVATION REPORT (RANDOM NUMBER R_1, PROGRAM ID,

AND UNIT PRICE ATTACHED)

S27: UPDATE CUMULATIVE UNIT PRICES

S29: ENCRYPT RANDOM NUMBER R_1 (ENCRYPTION KEY K)

S31: TRANSMIT ENCRYPTED RANDOM NUMBER $K(R_1)$

S33: RECEIVE ENCRYPTED RANDOM NUMBER $K(R_1)$

S35: DECRYPT ENCRYPTED RANDOM NUMBER $K(R_1)$ (DECRYPTION KEY K')

S37: VERIFY COINCIDENCE BETWEEN DECRYPTED RANDOM NUMBER R_1' AND GENERATED RANDOM NUMBER R_1

FIG. 5

1: CHECK POINT FUNCTION

2: USAGE RECORDING MODULE

3: CHARGING SERVER APPARATUS

S41: GENERATE RANDOM NUMBER R_2

S43: ENCRYPT RANDOM NUMBER R_2 AND USAGE RECORD U (PUBLIC KEY Ks)

S45: TRANSMIT ENCRYPTED INFORMATION Ks (R_2, U)

S47: RECEIVE ENCRYPTED INFORMATION Ks (R_2, U)

S49: DECRYPT ENCRYPTED INFORMATION Ks (R_2, U) (PRIVATE KEY Ks^{-1}

S51: UPDATE CHARGING INFORMATION

S53: ENCRYPT RANDOM NUMBER R_2 (PRIVATE KEY Ks^{-1})

S55: TRANSMIT ENCRYPTED RANDOM NUMBER $Ks^{-1}(R_2)$

S57: RECEIVE ENCRYPTED RANDOM NUMBER $Ks^{-1}(R_2)$

S59: DECRYPT ENCRYPTED RANDOM NUMBER $Ks^{-1}(R_2)$ (PUBLIC KEY Ks)

S61: VERIFY COINCIDENCE BETWEEN DECRYPTED RANDOM NUMBER R_2'

AND GENERATED RANDOM NUMBER R_2

S63: DELETE USAGE RECORD U